

## AMENDMENTS TO CLAIMS

1. (currently amended): A system ~~for encrypting a portion of token data, for recording said token data with a portion of said token data in an encrypted form on a computer readable medium, and for reading said token data and decrypting said portion of said token data, wherein said system comprises~~ comprising a plurality of client computers, and a server separate from the plurality of client computers, and a plurality of computer readable media, wherein

each computer readable medium within said plurality of computer readable media is transportable to each client computer in said plurality of client computers and is readable and writable within each client computer in said plurality of client computers,

said server generates a secure transfer key pair and encrypts a private key of said secure transfer key pair,

said secure transfer key pair is transferred to each of said client computers in said plurality thereof with said private key of said secure transfer key pair in an encrypted form, and

each client computer in said plurality thereof is programmed to generate token data including said portion of said token data encrypted with a public key of said secure transfer key pair, to record said token data on a computer readable medium in said plurality of computer readable media, to read said token data from ~~said a computer readable medium~~ in said plurality of computer readable media, to decrypt said private key of said secure transfer key pair, and to decrypt said portion of said token data with said private key of said secure transfer key pair, and to be enabled to perform a predetermined task after decrypting said portion of said token data.

2. (previously presented): The system of claim 1, wherein

each client computer in said plurality thereof generates a platform key pair,

4           a public key of said platform key pair is transferred to said server, and  
5           said secure transfer key pair is transferred to each of said client  
6 computers in said plurality thereof with said private key of said secure transfer  
7 key pair encrypted with said public key of said platform key pair of said client  
8 computer, and each client computer in said plurality thereof stores said secure  
9 transfer key pair with said private key of said secure transfer key pair encrypted  
10 with said public key of said platform key pair and subsequently decrypts said  
11 private key of said secure transfer key pair with said private key of said platform  
12 key pair.

1       3. (original): The system of claim 2, wherein  
2           each client computer in said plurality thereof includes a security  
3 subsystem having a subsystem processor and subsystem storage,  
4           each client computer in said plurality thereof generates a hardware key  
5 pair within said security subsystem  
6           a private key of said hardware key pair is stored in said subsystem  
7 storage, and  
8           a private key of said platform key pair is encrypted with said hardware  
9 public key and is decrypted with said hardware private key in said security  
10 subsystem before said private key of said platform key pair is used to decrypt  
11 said private key of said secure transfer key pair within said security subsystem.

1       4. (canceled)

1       5. (original): The system of claim 1, wherein  
2           each client computer in said plurality of client computers includes an input  
3 device for providing a numeric input,  
4           said portion of said token data includes a PIN,  
5           each client computer in said plurality of client computers, after decrypting  
6 said portion of said token data read from said computer readable medium,

7 compares said PIN included within said token data with said numeric input  
8 provided through said input device, and

9 each of said client computers in said plurality thereof reads said secure  
10 transfer key pair with said private key of said secure transfer key pair in said  
11 encrypted form from said computer readable medium.

1 9. (previously presented): The system of claim 8, wherein

2 each client computer in said plurality thereof generates a platform key pair  
3 and writes a public key of said platform key pair on a first computer readable  
4 medium,

5 said server reads said public key of said platform key pair from each client  
6 computer in said plurality thereof, encrypts said private key of said secure  
7 transfer key pair with said public key of said platform key pair, and writes said  
8 secure transfer key pair on a second computer readable medium with said  
9 private key of said secure transfer key pair encrypted with said public key of said  
10 client computer, and

11 said client computer reads said secure transfer key pair with said private  
12 key so said secure transfer key pair encrypted with said public key of said client  
13 computer from said second computer readable medium, stores said secure  
14 transfer key pair with said private key of said secure transfer key pair encrypted  
15 with said public key of said platform key pair and subsequently decrypts said  
16 private key of said secure transfer key pair with said private key of said platform  
17 key pair.

1 10. (currently amended): A method within a computing system for generating a  
2 token causing a computer system in a plurality of computer systems to be  
3 enabled to perform a predetermined task and for reading a token to be enabled  
4 to perform a predetermined task ~~for encrypting token data, for recording said~~  
5 ~~token data in an encrypted form on a computer readable medium, and for~~

6 ~~reading and decrypting token data recorded on a computer readable medium,~~  
7 wherein said method comprises:

8 receiving a secure transfer key pair generated within a server separate  
9 from said plurality of computer systems;

10 storing said secure transfer key pair;

11 after storing said secure transfer key pair, in response to an indication  
12 that token data is to be recorded, encrypting a portion of said token data with a  
13 public key of said secure transfer key pair; and recording said token data,  
14 including said portion of said token data encrypted with said public key of said  
15 secure transfer key pair on a computer readable medium; ~~and~~

16 after storing said secure transfer key pair, in response to an indication that  
17 token data is to be read, reading said token data from a computer readable  
18 medium, and decrypting a portion of said data with a private key of said secure  
19 transfer key pair, and

20 being enabled to perform a predetermined task after decrypting said  
21 portion of said data.

1 11. (original): The method of claim 10, wherein said secure transfer key pair is received  
2 from said server over a communications network.

1 12. (original): The method of claim 11, additionally comprising:

2 generating and storing a platform key pair;

3 transmitting a public key of said platform key pair to said server over said  
4 communications network, wherein said secure transfer key pair is subsequently  
5 received from said server encrypted with said public key of said platform key pair,  
6 and wherein said private key of said secure transfer key pair is stored encrypted  
7 with said public key of said platform key pair, and

8 decrypting said private key of said secure transfer key pair with said  
9 private key of said platform key pair before decrypting said portion of said data  
10 with said private key of said secure transfer key pair.

1 13. (original): The method of claim 10, wherein said secure transfer key pair is  
2 read from a computer readable medium.

1 14. (previously presented): The method of claim 13, additionally comprising:

2 generating and storing a platform key pair;

3 writing a public key of said platform key pair on a computer readable  
4 medium;

5 reading said secure transfer key pair from a computer readable medium  
6 encrypted with said public key of said platform key pair, wherein said private  
7 key of said secure transfer key pair is stored encrypted with said public key of  
8 said platform key pair; and

9 decrypting said private key of said secure transfer key pair with said  
10 private key of said platform key pair before decrypting said portion of said data  
11 with said private key of said secure transfer key pair.

1 15. (original): The method of claim 10, additionally comprising:

2 generating and storing a hardware key pair within a security subsystem of  
3 said computing system, wherein a private key of said hardware key pair is stored  
4 within said security subsystem of said computing system;

5 encrypting said private key of said platform key pair with said public key of  
6 said hardware key pair, wherein said platform key pair is stored with said private  
7 key of said platform key pair encrypted with said public key of said hardware key  
8 pair; and

9 decrypting said private key of said platform key pair with said private key  
10 of said hardware key pair within said security subsystem before decrypting said  
11 private key of said secure transfer key pair with said private key of said platform  
12 key pair.

1 16. (original): The method of claim 10, additionally comprising enabling  
2 performance of a predetermined task in response to decrypting said portion of  
3 said data with said private key of said secure transfer key pair.

1 17. (original): The method of claim 10, wherein  
2 said portion of said token data includes a PIN, and  
3 said method additionally comprises receiving a numeric input from an  
4 input device, comparing said PIN with said numeric input from said input device,  
5 and enabling performance of a predetermined task in response to determining an  
6 equivalence between said PIN and said numeric input.

1 18. (currently amended): A computer readable medium having recorded  
2 thereon computer executable instructions for performing a method within a  
3 computing system for generating a token causing a computer system in a  
4 plurality of computer systems to be enabled to perform a predetermined task  
5 and for reading a token to be enabled to perform a predetermined task  
6 ~~encrypting token data, for recording said token data in an encrypted form on a~~  
7 ~~computer readable medium, and for reading and decrypting token data recorded~~  
8 ~~on a computer readable medium~~, wherein said method comprises:  
9 receiving a secure transfer key pair from a server separate from said  
10 plurality of computer systems;  
11 storing said secure transfer key pair;  
12 after storing said secure transfer key pair, in response to an indication that  
13 token data is to be recorded, encrypting a portion of said token data with a public  
14 key of said secure transfer key pair[[:]] and recording said token data, including said  
15 portion of said token data encrypted with said public key of said secure transfer  
16 key pair on a computer readable medium; and  
17 after storing said secure transfer key pair, in response to an indication that  
18 token data is to be read, reading said token data from a computer readable  
19 medium, and decrypting a portion of said data with a private key of said secure

20 transfer key pair, and  
21 being enabled to perform a predetermined task after decrypting said  
22 portion of said data.

1 19. (original): The computer readable medium of claim 18, wherein said secure transfer  
2 key pair is received from said server over a communications network.

1 20. (original): The computer readable medium of claim 19, wherein said method  
2 additionally comprises:  
3 generating and storing a platform key pair;  
4 transmitting a public key of said platform key pair to said server over said  
5 communications network, wherein said secure transfer key pair is subsequently  
6 received from said server encrypted with said public key of said platform key pair,  
7 and wherein said private key of said secure transfer key pair is stored encrypted  
8 with said public key of said platform key pair, and  
9 decrypting said private key of said secure transfer key pair with said  
10 private key of said platform key pair before decrypting said portion of said data  
11 with said private key of said secure transfer key pair.

1 21. (original): The computer readable medium of claim 18, wherein said secure  
2 transfer key pair is read from a computer readable medium.

1 22. (previously presented): The computer readable medium of claim 21, wherein  
2 said method additionally comprises:  
3 generating and storing a platform key pair;  
4 writing a public key of said platform key pair on a computer readable  
5 medium;  
6 reading said secure transfer key pair from a computer readable medium  
7 encrypted with said public key of said platform key pair, wherein said private  
8 key of said secure transfer key pair is stored encrypted with said public key of

9       said platform key pair; and  
10            decrypting said private key of said secure transfer key pair with said  
11       private key of said platform key pair before decrypting said portion of said data  
12       with said private key of said secure transfer key pair.

1       23. (original): The computer readable medium of claim 18, wherein said method  
2       additionally comprises:

3            generating and storing a hardware key pair within a security subsystem of  
4       said computing system, wherein a private key of said hardware key pair is stored  
5       within said security subsystem of said computing system;

6            encrypting said private key of said platform key pair with said public key  
7       of said hardware key pair, wherein said platform key pair is stored with said  
8       private key of said platform key pair encrypted with said public key of said  
9       hardware key pair; and

10          decrypting said private key of said platform key pair with said private key  
11       of said hardware key pair within said security subsystem before decrypting said  
12       private key of said secure transfer key pair with said private key of said platform  
13       key pair.

1       24. (original): The computer readable medium of claim 18, wherein said method  
2       additionally comprises enabling performance of a predetermined task in  
3       response to decrypting said portion of said data with said private key of said  
4       secure transfer key pair.

1       25. (original): The computer readable medium of claim 18, wherein:  
2            said portion of said token data includes a PIN, and  
3            said method additionally comprises receiving a numeric input from an  
4       input device, comparing said PIN with said numeric input from said input device,  
5       and enabling performance of a predetermined task in response to determining an  
6       equivalence between said PIN and said numeric input.



1 26. (currently amended): A process of providing electrical signals over a  
2 communications network causing computer storage to have stored therein  
3 computer executable instructions for performing a method within a computing  
4 system for encrypting token data, for generating a token causing a computer  
5 system in a plurality of computer systems to be enabled to perform a  
6 predetermined task and for reading a token to be enabled to perform a  
7 predetermined task ~~for recording said token data in an encrypted form on a~~  
8 ~~computer readable medium, and for reading and decrypting token data recorded~~  
9 ~~on a computer readable medium~~, wherein said method comprises:

10 receiving a secure transfer key pair from a server separate from said  
11 computer system;

12 storing said secure transfer key pair;

13 after storing said secure transfer key pair, in response to an indication that  
14 token data is to be recorded, encrypting a portion of said token data with a public  
15 key of said secure transfer key pair; and recording said token data, including said  
16 portion of said token data encrypted with said public key of said secure transfer  
17 key pair on a computer readable medium; ~~and~~

18 after storing said secure transfer key pair, in response to an indication that  
19 token data is to be read, reading said token data from a computer readable  
20 medium, and decrypting a portion of said data with a private key of said secure  
21 transfer key pair, and

22 being enabled to perform a predetermined task after decrypting said  
23 portion of said data.

1 27. (original): The process of claim 26, wherein said secure transfer key pair is received  
2 from said server over a communications network.

1 28. (original): The process of claim 27, wherein said method additionally  
2 comprises:

3       generating and storing a platform key pair;  
4       transmitting a public key of said platform key pair to said server over said  
5 communications network, wherein said secure transfer key pair is subsequently  
6 received from said server encrypted with said public key of said platform key pair,  
7 and wherein said private key of said secure transfer key pair is stored encrypted  
8 with said public key of said platform key pair, and  
9       decrypting said private key of said secure transfer key pair with said  
10 private key of said platform key pair before decrypting said portion of said data  
11 with said private key of said secure transfer key pair.

1 29. (original): The process of claim 26, wherein said secure transfer key pair is read  
2 from a computer readable medium.

1 30. (currently amended): The process of claim 29, additionally comprising:  
2 generating and storing a platform key pair;

3       writing a public key of said platform key pair on a computer readable  
4 medium,

5       reading said secure transfer key pair from a computer readable medium  
6 encrypted with said public key of said platform key pair, and wherein said private  
7 key of said secure transfer key pair is stored encrypted with said public key of  
8 said platform key pair, and

9       decrypting said private key of said secure transfer key pair with said  
10 private key of said platform key pair before decrypting said portion of said data  
11 with said private key of said secure transfer key pair.

1 31. (original): The process of claim 26, wherein said method additionally comprises:

2       generating and storing a hardware key pair within a security subsystem of  
3 said computing system, wherein a private key of said hardware key pair is stored

4 within said security subsystem of said computing system;  
5 encrypting said private key of said platform key pair with said public key of  
6 said hardware key pair, wherein said platform key pair is stored with said private  
7 key of said platform key pair encrypted with said public key of said hardware key  
8 pair; and  
9 decrypting said private key of said platform key pair with said private key  
10 of said hardware key pair within said security subsystem before decrypting said  
11 private key of said secure transfer key pair with said private key of said platform  
12 key pair.

1 32. (original): The process of claim 26, wherein said method additionally  
2 comprises enabling performance of a predetermined task in response to  
3 decrypting said portion of said data with said private key of said secure transfer  
4 key pair.

1 33. (original): The process of claim 26, wherein:  
2 said portion of said token data includes a PIN, and  
3 said method additionally comprises receiving a numeric input from an  
4 input device, comparing said PIN with said numeric input from said input device,  
5 and enabling performance of a predetermined task in response to determining an  
6 equivalence between said PIN and said numeric input.

1 34. (currently amended): A method for enabling performance of [[a]]  
2 predetermined task tasks in a local computer and in a remote computer system  
3 through use of an encrypted portion of token data recorded in a the local  
4 computer, wherein said method comprises:  
5 generating a secure transfer key pair within a server separate from said  
6 local computer and from said remote computer;  
7 transferring said secure transfer key pair from said server to said local  
8 computer;

9 storing said secure transfer key pair within said local computer;  
10 establishing communication between said remote computer and said  
11 server;  
12 transferring said secure transfer key pair from said server to said remote  
13 computer;  
14 storing said secure transfer key pair within said remote computer;  
15 encrypting said portion of said token data within said local computer with a  
16 public key of said secure transfer key pair;  
17 recording said token data, including said portion of said token data  
18 encrypted with said public key of said secure transfer key pair, within said local  
19 computer on a computer readable medium;  
20 reading said token data, including said portion of said token data  
21 encrypted with said public key of said secure transfer key pair, within said secure  
22 transfer key pair, within said remote computer from said computer readable  
23 medium;  
24 decrypting said portion of said token data within said local computer with  
25 a private key of said secure transfer key pair;  
26 enabling said performance of a predetermined task within said local  
27 computer in response to decrypting said portion of said token data;  
28 transporting said computer readable medium from said local computer to  
29 said remote computer; reading said token data, including said portion of said  
30 token data encrypted with said public key of said secure transfer key pair, within  
31 said remote computer from a said computer readable medium;  
32 decrypting said portion of said token data within said remote computer  
33 with a private key of said secure transfer key pair; and  
34 enabling said performance of ~~said~~ a predetermined task in said remote  
35 computer in response to decrypting said portion of said token data.

1 35. (previously presented): The method of claim 34, wherein said secure  
2 transfer key pair is received from said server over a communications network.

1 36. (original): The method of claim 34, additionally comprising:

2 generating and storing a first platform key pair within said local computer;

3 and

4 transmitting a public key of said first platform key pair to said server from  
5 said local computer, wherein said secure transfer key pair is subsequently  
6 received by said local computer from said server encrypted with said public key  
7 of said first platform key pair, and wherein said private key of said secure transfer  
8 key pair is stored within said local computer encrypted with said public key of  
9 said first platform key pair.

1 37. (original): The method of claim 34, wherein said secure transfer key pair is  
2 read from a computer readable medium.

1 38. (original): The method of claim 37, wherein said method additionally  
2 comprises:

3 generating and storing a platform key pair;  
4 writing a public key of said platform key pair on a computer readable  
5 medium,  
6 reading said secure transfer key pair from a computer readable medium  
7 encrypted with said public key of said platform key pair, and wherein said private  
8 key of said secure transfer key pair is stored encrypted with said public key of  
9 said platform key pair, and  
10 decrypting said private key of said secure transfer key pair with said  
11 private key of said platform key pair before decrypting said portion of said data  
12 with said private key of said secure transfer key pair.

1 39. (original): The method of claim 34, additionally comprising:

2 generating and storing a first hardware key pair in a security subsystem of  
3 said local computer, wherein a private key of said hardware key pair is stored

4 within said security subsystem of said local computer;  
5 encrypting said private key of said first platform key pair with said public  
6 key of said first hardware key pair within said local computer, wherein said first  
7 platform key pair is stored within said local computer with said private key of said  
8 first platform key pair encrypted with said public key of said first hardware key  
9 pair.

1 40. (original): The method of claim 34, additionally comprising:

2 generating and storing a second platform key pair within said remote  
3 computer;

4 transmitting a public key of said second platform key pair to said server  
5 from said remote computer, wherein said secure transfer key pair is  
6 subsequently received by said remote computer from said server encrypted with  
7 said public key of said second platform key pair, and wherein said private key of  
8 said secure transfer key pair is stored within said remote computer encrypted  
9 with said public key of said second platform key pair, and

10 decrypting said private key of said secure transfer key pair with said  
11 private key of said second platform key pair within said remote computer before  
12 decrypting said portion of said data with said private key of said secure transfer  
13 key pair.

1 41. (original): The method of claim 34, additionally comprising:

2 generating and storing a second hardware key pair within a security  
3 subsystem of said remote computer, wherein a private key of said hardware key  
4 pair is stored within said security subsystem of said remote computer;

5 encrypting said private key of said second platform key pair with said  
6 public key of said second hardware key pair within said remote computer,  
7 wherein said second platform key pair is stored within said remote computer with  
8 said private key of said second platform key pair encrypted with said public key  
9 of said second hardware key pair; and

10 decrypting said private key of said second platform key pair with said  
11 private key of said second hardware key pair within said security subsystem of  
12 said remote computer before decrypting said private key of said secure transfer  
13 key pair with said private key of said second platform key pair.

1 42. (canceled)

1 43. (original): The method of claim 36, wherein  
2 said portion of said token data encrypted with said public key of said  
3 secure transfer key pair includes a PIN, and  
4 said method additionally comprises receiving a numeric input within said  
5 remote computer from an input device, comparing said PIN with said numeric  
6 input from said input device, and enabling performance of a predetermined task  
7 within said remote computer in response to determining an equivalence between  
8 said PIN and said numeric input.

1 44. (currently amended): A method for establishing a plurality of associated  
2 client computers, wherein a client computer in said plurality of associated client  
3 computers performs a predetermined task in response to reading and decrypting  
4 token data recorded on a computer readable medium, wherein said method  
5 comprises:

6 generating a secure transfer key pair within a server separate from said  
7 plurality of associated client computers;

8 transferring said secure transfer key pair from said server to each client  
9 computer in said plurality of associated client computers;

10 storing said secure transfer key pair within each client computer in said  
11 plurality of associated client computers;

12 encrypting a first portion of token data with a public key of said secure  
13 transfer key pair within a first client computer within said plurality of associated  
14 client computers;

15            recording token data on a computer readable medium, wherein said token  
16 data includes said first portion of token data encrypted with said public key of  
17 said secure transfer key pair, in said first client computer;  
18            transferring said computer readable medium from said first client  
19 computer to a second client computer within said plurality of associated client  
20 computers; reading said token data on said second client computer; and  
21            decrypting said token data encrypted with said public key of said secure  
22 transfer key pair with a private key of said secure transfer key pair in said second  
23 client computer.

1        45. (original): The method of claim 44, wherein  
2            each client computer within said plurality of associated client computers  
3 generates a platform key pair,  
4            a public key of said platform key pair is transferred from said client  
5 computer to said server,  
6            said private key of said secure transfer key pair is encrypted within said  
7 server with said public key of said platform key pair,  
8            said secure transfer key pair is transferred from said server to said client  
9 computer with a private key of said secure transfer key pair encrypted with said  
10 public key of said platform key pair.

1        46. (original): The method of claim 45, wherein said secure transfer key pair is  
2 transferred from said server to said client computer on a computer readable  
3 medium.

1        47. (original): The method of claim 45, wherein said secure transfer key pair is  
2 transferred from said server to said client computer by transmission over a  
3 communications network.



1 48. (original): The method of claim 45, additionally comprising:

2 generating and storing a hardware key pair within a security subsystem of  
3 said client system, wherein a private key of said hardware key pair is stored  
4 within said security subsystem of said client computer;

5 encrypting said private key of said platform key pair with said public key of  
6 said hardware key pair, wherein said platform key pair is stored with said private  
7 key of said platform key pair encrypted with said public key of said hardware key  
8 pair; and

9 decrypting said private key of said platform key pair with said private key  
10 of said hardware key pair within said security subsystem before decrypting said  
11 private key of said secure transfer key pair with said private key of said platform  
12 key pair.

1 49. (original): The method of claim ~~40~~ 45, wherein

2 a portion of said token data includes a PIN, and  
3 said method additionally comprises receiving a numeric input from an input  
4 device, comparing said PIN with said numeric input from said input device, and  
5 enabling performance of a predetermined task in response to determining an  
6 equivalence between said PIN and said numeric input.

1 50. (currently amended): A method for establishing a plurality of associated  
2 client computers, wherein a client computer in said plurality of associated client  
3 computers performs a predetermined task in response to reading and decrypting  
4 token data recorded on a computer readable medium, wherein said method  
5 comprises:

6 generating a secure transfer key pair within a server separate from said  
7 plurality of associated client computers;

8 transferring said secure transfer key pair from said server to each client  
9 computer in said plurality of associated client computers; and

10 storing said secure transfer key pair within each client computer in said  
11 plurality of associated client computers.

1 51. (original): The method of claim 50, wherein  
2 said method additionally comprises receiving a platform key pair from said  
3 client computer within said plurality of associated client computers before  
4 transferring said secure transfer key pair to said client computer,  
5 said secure transfer key pair is transferred from said server to said client  
6 computer with a private key of said secure transfer key pair encrypted with said  
7 public key of said platform key pair.

1 52. (original): The method of claim 51, wherein said secure transfer key pair is  
2 transferred from said server to said client computer over a communications  
3 network.

1 53. (original): The method of claim 51, wherein said secure transfer key pair is  
2 transferred from said server to said client computer as data recorded on a  
3 computer readable medium.